CLAIMS

1. A method of reliably identifying a user in a computer system, in which method a mobile station is used for communicating with the computer system and a personal identification number is supplied into the mobile station, the method comprising the steps of:

generating a first one-time password in the mobile station without any action by the user by utilizing a known algorithm on the basis of a personal identification number of the user, subscriber-specific identifier read from a subscriber-specific identification module of the mobile station, device-specific identifier of the mobile station and time,

encoding the first one-time password and the subscriber-specific identifier of the user at the mobile station,

transmitting the encoded password and subscriber-specific identifier to an authentication server of the computer system,

identifying the user at the authentication server on the basis of the subscriber-specific identifier, and

searching a database for the personal identifier number of the user and the device-specific identifier of the mobile station associated with the user,

generating a second one-time password at the authentication server by utilizing the predetermined algorithm on the basis of the personal identification number of the user, subscriber-specific identifier, device-specific identifier of the mobile station and time,

comparing the first password and the second password with each other at the authentication server, and if the passwords match,

enabling the telecommunication connection between the mobile station of the user and the computer system.

2. A method as claimed in claim 1, wherein the mobile station synchronizes the timimg of the mobile station with the timing of the authentication server before the identification procedure is started.

3. A method as claimed in claim 1, wherein the user is identified automatically when the user starts an application utilizing the computer system in the mobile station.

4. A method as claimed in claim 1, wherein the authentication server transmits no information to the mobile station if the first and the second passwords do not match.

5. A method as claimed in claim 1, wherein during the identification, the terminal transmits to the authentication server a message comprising at least a field comprising a SRES value, a field comprising time, a field comprising an international telephone number of the terminal, and a field comprising a device number of the terminal.

6. A method as claimed in claim 1, wherein during the identification, a PPP/CHAP protocol is used in connection with a RADIUS protocol, and the terminal transmits to the authentication server a message comprising at least a field comprising a SRES value, a field comprising a user name to the system, and a field comprising a password generated from a device identifier, subscriber-specific identifier of the user, personal identification number of the user, time and the SRES value.

7. A method as claimed in claim 1, wherein during the identification, a PPP/PAP protocol is used in connection with the RADIUS protocol, and the terminal transmits to the authentication server a message comprising at least a field comprising a password generated from the device identifier, subscriber-specific identifier of the user, personal identification number of the user, time, and SRES value, a field comprising a SRES value, and a field comprising a user number to the system.

8. A method as claimed in ~~any one of preceding claims 1 to 7~~ claim 1, wherein information necessary for encryption is stored in the terminal in more than one subscriber-specific identification module.

9. A method as claimed in claim 6 ~~or 7~~, wherein the user name to the system is the user's MSISDN.

10. An arrangement for reliably identifying a user in a computer system, which arrangement comprises

a mobile station used for communicating with the computer system, the mobile station comprising

a subscriber-specific identification module comprising a subscriber-specific identifier,

a device-specific identifier permanently encoded in the mobile station,

means for reading a personal identifier number which is supplied by the user and which enables the device to be used,

means for checking the correctness of the identifier number always before the device is put to use, and

which arrangement comprises an authentication server comprising

memory means for storing the user names of the users in the system and the corresponding personal identifiers and device-specific identifiers,

the mobile station further comprising

means for generating a first one-time password without any action by the user by utilizing a known algorithm on the basis of the personal identification number of the user, subscriber-specific identifier read from a subscriber-specific identification module of the mobile station, device-specific identifier of the mobile station and time,

means for encoding the first one-time password and the subscriber-specific identifier of the user,

means for transmitting the encoded password and subscriber-specific identifier to an authentication server of the computer system, and the authentication server is further arranged to

identify the user on the basis of the subscriber-specific identifier, and search a database for the personal identifier number of the user and the device-specific identifier of the mobile station associated with the user,

generate a second one-time password at the authentication server by utilizing the predetermined algorithm on the basis of the personal identification number of the user, subscriber-specific identifier, device-specific identifier of the mobile station and time,

compare the first password and the second password with each other at the authentication server, and if the passwords match, enable the telecommunication connection between the mobile station of the user and the computer system.

11. An arrangement as claimed in claim 10, wherein the mobile station is arranged to synchronize the timimg of the mobile station with the timing of the authentication server before the identification procedure is started.

12. An arrangement as claimed in claim 10, wherein the mobile station is arranged to identify the user automatically when the user starts an application utilizing the computer system in the mobile station.

13. An arrangement as claimed in claim 10, wherein the authentication server is arranged not to transmit any information to the mobile station if the first and the second passwords do not match.

14. An arrangement as claimed in claim 10, wherein the mobile station is arranged to transmit to the authentication server a message comprising

at least a field comprising a SRES value, a field comprising time, a field comprising an international telephone number of the terminal, and a field comprising a device number of the terminal.

15. An arrangement as claimed in claim 10, wherein the mobile station and the authentication server are arranged to use a PPP/CHAP protocol in connection with a RADIUS protocol during the identification, and the terminal is arranged to transmit to the authentication server a message comprising at least a field comprising a SRES value, a field comprising a user name to the system, and a field comprising a password generated from a device identifier, subscriber-specific identifier of the user, personal identification number of the user, time and the SRES value.

16. An arrangement as claimed in claim 10, wherein the mobile station and the authentication server are arranged to use a PPP/PAP protocol in connection with the RADIUS protocol during the identification, and the mobile station is arranged to transmit to the authentication server a message comprising at least a field comprising a password generated from the device identifier, subscriber-specific identifier of the user, personal identification number of the user, time, and SRES value, a field comprising a SRES value, and a field comprising a user number to the system.

17. An arrangement as claimed in ~~claims 15 or 16~~ claim 15, wherein the user name to the system is the user's MSISDN.

18. An arrangement as claimed in ~~any one of preceding claims 10 to 17~~ claim 10, wherein the mobile station is a GPRS system mobile station.

19. An arrangement as claimed in ~~any one of preceding claims 10 to 17~~ claim 10, wherein the mobile station comprises more than one subscriber-specific identification module, and information necessary for encryption is stored in more than one identification module.